



Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at <http://about.jstor.org/participate-jstor/individuals/early-journal-content>.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

Concerning an Analogy Between Formal Modular Invariants and the Class of Algebraical Invariants Called Booleans.

BY O. E. GLENN.

In the general theory of algebraic invariants and covariants the coefficients of the forms involved are considered to be arbitrary variables. Likewise the coefficients in the set of linear transformations to which the forms are subjected are arbitrary variable parameters.

Hurwitz published, in 1903, a paper* in which he defined a type of invariant essentially different from the ordinary algebraic type. The distinction consists in this: Whereas the coefficients of the forms are still arbitrary variables, the coefficients of the linear transformations involved are parameters representing integers belonging to the residue system modulo p , p being a prime number.

Professor L. E. Dickson has called my attention to the present state of this theory. No proof of the finiteness of the formal modular concomitants described above has been published. Hurwitz has emphasized the difficulty of this problem in the case of the invariants.

In a recent paper Miss Sanderson proves a fundamental relation between the formal modular type and *modular*† invariants and covariants‡ as defined and extensively investigated by Dickson. The latter author has recently contributed a general invariant theory, the methods of which apply both to the modular and to the algebraic types of invariant. He has made applications of this method to the formal modular case.

§ 1. *Extension of a Principle Due to Boole.*

It is the purpose of this paper to show how a principle due to Boole,§ applied by him to the problem of finding a fundamental system of invariants and covariants of a binary form under the restricted substitutions

* Hurwitz, "Ueber höhere Kongruenzen," *Archiv der Math. und Phys.*, Ser. 3, Vol. V (1903).

† Dickson, *Transactions Amer. Math. Society*, Vol. X (1909) and Vol. XIV (1913); *AMERICAN JOURNAL OF MATHEMATICS*, Vol. XXXI (1909); *Proceedings London Math. Society*, Ser. 2, Vol. VII (1909); etc. An elementary account of Dickson's modular invariant and covariant theory and of his general invariant theory will be found in his "Colloquium Lectures," delivered at the Madison Colloquium of the American Mathematical Society in September, 1913.

‡ Sanderson, *Transactions Amer. Math. Society*, Vol. XIV (1913).

§ Boole, *Cambridge Mathematical Journal*, Vol. III.

$$x_1 = x'_1 \frac{\sin(\omega - \alpha)}{\sin \omega} + x'_2 \frac{\sin(\omega - \beta)}{\sin \omega}, \quad x_2 = x'_1 \frac{\sin \alpha}{\sin \omega} + x'_2 \frac{\sin \beta}{\sin \omega}, \quad (1)$$

may be applied in the case of formal modular concomitants.

The essential features of the method of Boole result from the fact that the form $f = x_1^2 + 2x_1x_2 \cos \omega + x_2^2$ is a universal covariant* under the transformation (1). That is,

$$x_1'^2 + 2x_1'x_2' \cos \omega' + x_2'^2 = x_1^2 + 2x_1x_2 \cos \omega + x_2^2,$$

where ω is the inclination of the old axes, and $\omega' = \beta - \alpha$. Then the Boolean concomitants of a binary n -ic F_n are precisely the simultaneous concomitants of f and F_n .

Likewise, if we possess for the restricted substitutions consisting of the general binary linear transformations with coefficients reduced modulo p , a universal covariant C , then the members of the simultaneous system of C and F_n will be, as a rule,† formal modular concomitants of F_n .

A fundamental system of universal covariants of the general linear transformations in m variables, with coefficients belonging to a general finite field, has been discovered by Dickson and published in his memoir, "A Fundamental System of Invariants of the General Modular Linear Group, with a Solution of the Form Problem," *Transactions of the American Mathematical Society*, Vol. XII (1911). In view of the principle explained above we may, in the present case, employ these universal covariants in place of C , restricting the finite field to the field of integers modulo p ; $m=2$. Results of this combination are given in §§ 3, 4, 5.

§ 2. *Defining Properties of Formal Concomitants; (a), (b), (c).*

The definitions formulated by Hurwitz relate to absolute formal modular invariants only. We define the covariants of a form as follows: Let F_n be a binary form of order n with arbitrary coefficients;

$$F_n = a_0 x_1^n + a_1 x_1^{n-1} x_2 + \dots + a_n x_2^n.$$

Let F_n , transformed by the general linear binary transformation with coefficients belonging to the field of integers modulo p , go over into

$$F'_n = a'_0 x_1'^n + a'_1 x_1'^{n-1} x_2' + \dots + a'_n x_2'^n.$$

Let $\rho \not\equiv 0 \pmod{p}$ be the modulus of the transformation. Then

(a) *Any function $F(a_0, a_1, \dots, a_n, x_1, x_2)$ of the coefficients and variables of F_n which identically satisfies the congruence*

$$F(a'_0, a'_1, \dots, a'_n, x'_1, x'_2) \equiv \rho^k F(a_0, a_1, \dots, a_n, x_1, x_2) \pmod{p},$$

* Study, *Leipz. Ber.*, XL (1897).

† Compare § 5.

will be called a formal modular covariant of F_n . It will be a relative covariant except when $\rho^k \equiv 1 \pmod{p}$, when it will be an absolute covariant.

Without loss of generality we may assume that F is homogeneous both in the variables and in the coefficients. If its order is zero, it is an invariant.

(b) *The weight w of a term of F , and the index k , order ω , and the degree i of F satisfy the following congruences:*

$$\left. \begin{aligned} in - \omega &\equiv 2k \\ in + \omega &\equiv 2w \end{aligned} \right\} \pmod{p-1}. \quad (2)$$

For under the particular substitution $x_1 = \lambda x'_1$, $x_2 = \lambda x'_2$ ($\lambda =$ a primitive root) of determinant λ^2 , we have $a'_r = \lambda^n a_r$, $x'_i = \lambda^{-1} x_i$, from which the first congruence readily follows. To prove the second, take $x_1 = x'_1$, $x_2 = \lambda x'_2$, whence $a'_r = \lambda^r a_r$, $x'_2 = \lambda^{-1} x_2$. Let a typical term of F be

$$T = a_r^p a_s^\sigma a_t^\tau \dots x_1^p x_2^{\omega-p}.$$

Then,

$$T' = \lambda^{rp+s\sigma+t\tau+\dots+p-\omega} T \equiv \lambda^k T \pmod{p}.$$

Hence,

$$2(w - \omega) \equiv in - \omega \pmod{p-1},$$

which proves the second congruence.

(c) *The annihilators δ of a formal invariant $\phi(a)$ of degree i are partial differential operators of order i .* In fact, if F_n is transformed into F'_n by the particular substitution $S: x_1 = x'_1 + tx'_2$, $x_2 = x'_2$ (t a residue mod p), then $\phi(a')$ may be expanded by Taylor's theorem;* and after powers of t are reduced by Fermat's theorem (mod p), the result takes the form†

$$\phi(a') - \phi(a) \equiv \delta' \phi(a) t + \frac{\delta'^2}{2} \phi(a) t^2 + \dots + \frac{\delta'^{p-1} \phi(a)}{p-1} t^{p-1} \pmod{p}.$$

Here δ' is an operator of order $> i$. Then a necessary and sufficient condition for the invariancy of ϕ under S is given by $\delta' \phi(a) = 0$. If in δ' we delete all partial derivatives of orders $> i$, we obtain an annihilator δ as described above. We give below the explicit form of δ for $n=2$, $i=4$, $p=3$.

$$\begin{aligned} \delta \phi(a) &\equiv 2a_0 \phi_{a_1} + a_1 \phi_{a_2} + 2a_0^2 \phi_{a_1 a_2} + a_0 a_1 \phi_{a_2^2} + \frac{4}{3} a_0^3 \phi_{a_1^3} + 2a_0^2 a_1 \phi_{a_1^2 a_2} \\ &\quad + (a_0^3 + a_0 a_1^2) \phi_{a_1 a_2^2} + \left(\frac{1}{6} a_1^3 + \frac{1}{2} a_0^2 a_1 \right) \phi_{a_2^3} + \frac{4}{3} a_0^4 \phi_{a_1^3 a_2} + 2a_0^3 a_1 \phi_{a_1^2 a_2^2} \\ &\quad + a_0^2 a_1^2 \phi_{a_1 a_2^3} + \frac{1}{3} a_0^4 \phi_{a_1 a_2^3} + \frac{1}{6} (a_0 a_1^3 + a_0^3 a_1) \phi_{a_2^4}. \end{aligned} \quad (3)$$

In this operator $\phi_{a_1 a_2^2} = \frac{\partial^3 \phi}{\partial a_1 \partial a_2^2}$, etc.

*The method is due to Dickson, who developed it for modular invariants in *Transactions Amer. Math. Society*, Vol. VIII (1907), p. 209. The essential point of difference is that in the present case there is no greatest value for i , and δ is more complicated.

† Cf. *Transactions Amer. Math. Society*, Vol. XV, p. 72, lemma in § 1.

For illustration, we determine all invariants of F_2 , of degree 4, modulo 3. These will be determined again by the method of § 1 (Cf. § 5, Table II). Let

$$\begin{aligned}\phi(a) = & A_1^{(0)} a_0^4 + A_1^{(2)} a_0^3 a_2 + A_2^{(2)} a_0^2 a_1^2 + A_1^{(4)} a_0^2 a_2^2 + A_2^{(4)} a_0 a_1^2 a_2 \\ & + A_3^{(4)} a_1^4 + A_1^{(6)} a_0 a_2^3 + A_2^{(6)} a_1^2 a_2^2 + A_1^{(8)} a_2^4.\end{aligned}$$

By formula (2) this is the general form of $\phi(a)$. Operating by δ we obtain

$$\left. \begin{aligned}A_2^{(4)} - A_3^{(4)} + A_1^{(6)} &\equiv 0; & A_1^{(4)} &\equiv A_2^{(4)}; & A_2^{(6)} &\equiv A_1^{(8)} \equiv 0; \\ A_1^{(2)} + A_2^{(2)} + A_1^{(4)} - A_3^{(4)} &\equiv 0\end{aligned} \right\} \pmod{3}.$$

Also, since $\phi(a)$ must remain unaltered by the substitution $(a_0 a_2) (-a_1 a_1)$, we have

$$A_1^{(0)} \equiv A_2^{(2)} \equiv 0; \quad A_1^{(2)} \equiv A_1^{(6)} \pmod{3}.$$

Hence,

$$\begin{aligned}\phi(a) &\equiv A_1^{(4)} (a_0^2 a_2^2 + a_0 a_1^2 a_2 - a_0^3 a_2 - a_0 a_2^3) + A_3^{(4)} (a_0^3 a_2 + a_1^4 + a_0 a_2^3) \\ &\equiv A_1^{(4)} J + A_3^{(4)} I.\end{aligned}$$

Two linearly independent formal modular invariants of degree 4 are thus I and J . One of these is reducible. In fact,

$$I + J \equiv D^2 \pmod{3},$$

where D is the discriminant of F_2 .

§ 3. *Universal Covariants in Two Variables.*

The universal covariants forming a fundamental system for the general binary linear group, modulo p , are two in number. They are (see § 1)

$$L = x_1^p x_2 - x_1 x_2^p, \quad Q = (x_1^{p^2} x_2 - x_1 x_2^{p^2}) \div L.$$

We now prove a theorem concerning Q . Let $J_1(f\phi)$ be the functional determinant of f and ϕ . Let $J_2(f\phi)$ be the functional determinant of J_1 and ϕ , or the second iteration of the functional determinant of f and ϕ . In ordinary notation for transvectants,

$$J_2 = ((f\phi)\phi).$$

In general, let J_k be the k -th iteration; that is,

$$J_k = (\dots \overbrace{(f\phi)\phi}^k \dots \phi).$$

Then we have

THEOREM: *The covariant Q is a modular covariant of L , and is precisely the $(p-2)$ -th iteration of the functional determinant of the Hessian of L and L itself, modulo p .*

In proof, let $H = (LL)^2$. Then,

$$J_1(HL) \equiv -2x_1^{3(p-1)} + x_1^{2(p-1)} x_2^{2(p-1)} + x_1^{p-1} x_2^{3(p-1)} - 2x_2^{3(p-1)} \pmod{p}.$$

Proceeding by induction, assume

$$J_{k-2}(HL) \equiv a_0^{(k)} x_1^{k(p-1)} + a_1^{(k)} x_1^{(k-1)(p-1)} x_2^{p-1} + \dots + a_k^{(k)} x_2^{k(p-1)} \pmod{p}.$$

Then,

$$+J_{k-1}(HL) \equiv \left| \begin{array}{c} \frac{\partial J_{k-2}}{\partial x_1} \\ \frac{\partial J_{k-2}}{\partial x_2} \end{array} \begin{array}{c} x_2^p \\ -x_1^p \end{array} \right| \equiv a_0^{(k+1)} x_1^{(k+1)(p-1)} + a_1^{(k+1)} x_1^{k(p-1)} x_2^{p-1} + \dots + a_{k+1}^{(k+1)} x_2^{(k+1)(p-1)} \pmod{p}. \quad (4)$$

From this congruence we obtain the recursion formula

$$a_h^{(k+1)} \equiv (k-h) a_h^{(k)} + (h-1) a_{h-1}^{(k)} \pmod{p}, \quad (h=0, 1, \dots, k+1). \quad (5)$$

Let us now define two new a numbers as follows:

$$a_{-1}^{(k)} \equiv 0; \quad a_{k+1}^{(k)} \equiv 0 \pmod{p}.$$

Then we obtain readily from (5)

$$\left. \begin{array}{l} a_0^{(k+1)} \equiv -\lfloor k, \quad a_{k+1}^{(k+1)} \equiv -\lfloor k \\ a_h^{(k+1)} \equiv +\lfloor k-h \quad (h=1, \dots, k) \end{array} \right\} \pmod{p}.$$

Assume $k=p-1$. Then by virtue of Wilson's theorem

$$J_{p-2}(HL) \equiv x_1^{p(p-1)} + x_1^{(p-1)(p-1)} x_2^{p-1} + \dots + x_2^{p(p-1)} \equiv Q \pmod{p},$$

which was to be proved.

Since, then, Q is a covariant of L , it suffices to employ L for C (§ 1) in obtaining by the method of § 1 the concomitants of F_n modulo p .

§ 4. Concomitants of F_3 Modulo 2.

Let F_3 be the general binary cubic form

$$F_3 = a_0 x_1^3 + 3a_1 x_1^2 x_2 + 3a_2 x_1 x_2^2 + a_3 x_2^3,$$

and let $p=2$. Then the fundamental system* of F_3 and L , taken from the algebraical standpoint, is a closed set, and the system of irreducible concomitants obtained from this set by deleting the members which are reducible, modulo 2, constitutes a formal system for F_3 modulo 2. No proof that this is a fundamental system is given in this paper, however. These irreducible concomitants† are given in Table I. All transvectants in the simultaneous system of F_3 and L not given in the table prove to be reducible. For instance,

$$(HQ) \equiv H + R^{(2)}Q, \quad (Q(F_3L)^2) \equiv C_2^{(1)} + R^{(1)}Q, \quad \pmod{2}.$$

§ 5. Concomitants of F_2 Modulo 3.

We give in Table II similar results for the case $p=3, n=2$. The mere process of transvection here sometimes fails to give a formal concomitant (mod 3), owing primarily to the fact that some of the numerical coefficients involved are divisible by the modulus. No proof that the system given by the method is or is not coextensive with the totality of formal concomitants of $f(=F_2)$ is here attempted. It is, however, worthy of note that we obtain by

* Faa di Bruno, Walter, "Theorie der binären Formen," p. 209.

† With each transvectant has been introduced the smallest numerical factor which has the effect of removing extraneous numerical factors when the concomitant is expressed in terms of the actual coefficients.

transvection between f and Q alone a complete set of concomitants, which, when reduced by Fermat's theorem, modulo 3, give the fundamental system of *modular* concomitants of f .^{*} These are (see Table II) $q, \Delta, f, L, Q, C_1, C_2, f_4$.

TABLE I.

Notation	Transvectant	Concomitant (mod 2)
$R^{(1)}$	$(F_3 L)^3$	$a_1 + a_2$
$R^{(2)}$	$(H Q)^2$	$a_0 a_3 + a_1 a_2$
$R^{(3)}$		$a_0(a_0 + a_1 + a_2 + a_3)a_3$
L		$x_1^2 x_2 + x_1 x_2^2$
Q	$(LL)^2$	$x_1^2 + x_1 x_2 + x_2^2$
F_3		$a_0 x_1^3 + a_1 x_1^2 x_2 + a_2 x_1 x_2^2 + a_3 x_2^3$
H	$(F_3 F_3)^2$	$(a_0 a_2 + a_1^2) x_1^2 + (a_0 a_3 + a_1 a_2) x_1 x_2 + (a_1 a_3 + a_2^2) x_2^2$
$C_1^{(1)}$	$(Q F_3)^2$	$(a_0 + a_1 + a_2) x_1 + (a_1 + a_2 + a_3) x_2$
$C_2^{(1)}$	$(F_3 L)^2$	$a_0 x_1^2 + (a_1 + a_2) x_1 x_2 + a_3 x_2^2$
$C_4^{(1)}$	$(F_3 L)$	$a_0 x_1^4 + (a_1 + a_2) x_1^2 x_2^2 + a_3 x_2^4$
$C_1^{(2)}$	$(H L)^2$	$(a_0 a_3 + a_1 a_2 + a_0 a_2 + a_1^2) x_1 + (a_0 a_3 + a_1 a_2 + a_1 a_3 + a_2^2) x_2$
$C_2^{(3)}$	$(H(F_3 L)^2)$	$(a_0^2 a_3 + a_0 a_2^2 + a_1^3 + a_1^2 a_2) x_1^2 + (a_0 a_3^2 + a_1^2 a_3 + a_1 a_2^2 + a_2^3) x_2^2$

TABLE II.

Notation	Transvectant	Concomitant (mod 3)
Δ	$(ff)^2$	$a_1^2 - a_0 a_2$
q	$(f^3 Q)^6$	$a_0^2 a_2 + a_0 a_2^2 + a_0 a_1^2 + a_1^2 a_2 - a_0^3 - a_2^3$
I	$(f^4 L^2)^8$	$a_0^3 a_2 + a_0 a_2^3 + a_1^4$
L		$x_1^3 x_2 - x_1 x_2^3$
Q	$((LL)^2 L)$	$x_1^6 + x_1^4 x_2^2 + x_1^2 x_2^4 + x_2^6$
f		$a_0 x_1^2 + 2a_1 x_1 x_2 + a_2 x_2^2$
f_4	$(fQ)^2$	$a_0 x_1^4 + a_1 x_1^3 x_2 + a_1 x_1 x_2^3 + a_2 x_2^4$
C_1	$(f^3 Q)^5$	$(a_0^2 a_1 - a_1^3) x_1^2 + (a_0 - a_2)(a_1^2 + a_0 a_2) x_1 x_2 + (a_1^3 - a_1 a_2^2) x_2^2$
C_2	$(f^2 Q)^4$	$(a_0^2 + a_1^2 - a_0 a_2) x_1^2 + a_1(a_0 + a_2) x_1 x_2 + (a_1^2 + a_2^2 - a_0 a_2) x_2^2$
C_3	$(fL^2)^2$	$a_0 x_1^6 + 2a_1 x_1^3 x_2^3 + a_2 x_2^6$
C_4	$(f^2 L^2)^4$	$(a_0^2 + a_1^2 - a_0 a_2) x_1^4 + 2a_1(a_0 + a_2)(x_1^3 x_2 + x_1 x_2^3) + (a_1^2 + a_2^2 - a_0 a_2) x_2^4$
C_6	$(f^3 L^2)^6$	$a_0^3 x_1^2 + 2a_1^3 x_1 x_2 + a_2^3 x_2^2$
C_6	$(f^4 L^2)^7$	$(a_0 a_1^3 - a_0^3 a_1) x_1^2 + (a_0 a_2^3 - a_0^3 a_2) x_1 x_2 + (a_1 a_2^3 - a_1^3 a_2) x_2^2$

UNIVERSITY OF PENNSYLVANIA, October, 1913.

^{*} Dickson, *Transactions Amer. Math. Society*, Vol. XIV (1913), p. 310.